

# **ALINK 300Mbps WiFi High Power Outdoor 5G Bridge / 2.4G Access Point**



## **User Manual**

Revision 1.4

## Revision History

---

Version	Date	Notes
1.0	Oct. 21, 2010	Initial Version
1.1	July 28, 2011	"Auto-reboot" feature added. Designed for situation of near-end AP cannot receive "alive message" from far-end AP in a certain period. Then this function will perform automatically at near-end AP without notice. The "alive message" is communicated between near-end & far-end AP via 5GHz bridge links.
1.2a	Feb. 20, 2012	Initial generic version for 802.11n BR & AP ODU
1.3	May 29, 2012	Updated according to V3.1 firmware features
1.4	Nov 13,2012	Updated according to V3.1.6 firmware features

# Introduction

The MIMO 2x2 Wireless Outdoor System (“**outdoor unit**” in the following paragraphs) consists of two concurrent running radios, one at 5GHz supporting 802.11a/n standard, and the other at 2.4GHz for 802.11b/g/n features. This outdoor AP supports Point-to-Point, Point to Multipoint, building-to-building communication, that the data rate is up to 150Mbps in HT-20 mode, or to 300 Mbps in HT-40 mode. The bridge function is most suitable for enterprises, campus or off-site locations that require LAN or Internet access without the availability of wired networks to extend network coverage up to 35Km.; and the 802.11 b/g/n radio is mainly for Access Point application to provide local wireless access to the Internet.

The outdoor unit offers different encryption mechanisms including WEP, and AES to ensure the communication security. For APs / Bridges connections, the MAC address authentication mechanism is provided.

The outdoor unit is designed for the outdoor environment and it is full weather proof against the most stringent condition. For further protection, the bridge and Power over Ethernet adapter are all with the built-in lightning protectors.

To meet the stringent outdoor application, the outdoor unit incorporates the patent technology to ensure the operation of the radio over the wide temperature. The built-in lightning protectors further ensure the radio and its accessories’ safety during the operation. Power over Ethernet design, mounting accessory and field installation kits ensure easy to use experience.

The outdoor unit is in a weatherproof enclosure for mounting outdoors and includes its own brackets for attaching to a wall, pole, radio mast, or tower structure. The unit powered through its Ethernet cable connection from a power injector module that installed indoors. The wireless bridge system offers a fast, reliable, and cost-effective solution for connectivity between remote Ethernet wired LANs or to provide Internet access to an isolated site. The system is also easy to install and operate, ideal for situations where a wired link may be difficult or expensive to deploy.

In addition, the outdoor unit offers full network management capabilities through an easy-to-use web interface, a command-line interface, and support for Simple Network Management Protocol (SNMP) tools.

## Key Features:

- 2x2 MIMO for both 5GHz (802.11n/a) and 2.4GHz (802.11n/b/g) Radios Platform
- High speed Wire and Wireless connectivity
- 300Mbps 802.11n/a wireless backhaul & 300Mbps 802.11n/b/g AP coverage
- IP68 rated enclosure for dust and water protection
- Wide operating temperature: -35°C to +70°C
- Built-In lightning protection circuits

# Table of Contents

1. MIMO 2x2 Wireless Outdoor Access Point System Hardware Feature .....	8
1.1 Hardware Outline .....	8
Product Features .....	8
Feature Highlight .....	9
1.2 Interface .....	10
1.2.1 External Antenna Connection .....	10
1.2.2 Power over Ethernet (PoE) & Cable Connection .....	11
1.2.3 Grounding .....	11
1.3 Product Warranty .....	11
1.4 Warranty Limitation .....	11
1.5 System Requirement .....	11
1.6 Feature Summary .....	11
2. Getting Started .....	13
2.1 Setup Local Area Connection on your PC .....	13
2.1.1 Start Network Configuration on your PC .....	13
2.2 Check access to the unit .....	15
2.3 Access to web pages .....	16
2.4 Basic Configuration .....	17
2.4.1 System Setting .....	17
2.4.2 System Information .....	20
2.4.3 Upgrade .....	21
2.4.4 Reboot .....	22
3. Configure 5GHz Bridge .....	23
3.1 Bridge Configuration .....	23
4. Bridge Security Setting .....	31
4.1 Bridge Security Setting - WEP .....	31
4.2 Bridge Security Setting – WPA .....	32
5. Network Management .....	34
5.1 5GHz Bridge Connection Status .....	34
5.1.1 RSSI .....	35
6. Configure 2.4GHz AP .....	36
6.1 AP Configuration .....	36
6.2 AP Connection Status .....	37
7. Planning Linkage .....	42
7.1 Site Survey .....	42
7.2 Planning Radio Path .....	42
7.2.1 Antenna Height .....	44

## Table of Figures

Figure 1. Outdoor unit Hardware Outline .....	8
Figure 2. Antenna connection& bracket kit.....	10
Figure 3. PoE connection.....	11
Figure 4. Windows Start Menu.....	13
Figure 5. Network Connections.....	13
Figure 6. Local Area Connection Properties .....	11
Figure 7. Internet Protocol Properties.....	15
Figure 8. Ping& ARP command.....	16
Figure 9. User Name and Password Page.....	16
Figure 10. System Setting page .....	17
Figure 11. System Information page .....	19
Figure 12. Upgrade page .....	20
Figure 13. Reboot page .....	22
Figure 14. 5GHz radio basic setting page .....	23
Figure 15. Wireless mode page .....	24
Figure 16. Channel page.....	25
Figure 17. Data Rate page .....	27
Figure 18. Bridge mode page .....	27
Figure 19. Remote bridge setup page .....	28
Figure 20. Security page.....	29
Figure 21. Bridge security page - WEP .....	31
Figure 22. Bridge Security page - WPA .....	33
Figure 23. Master/Slave Bridges connection status .....	34
Figure 24. Master/Slave Bridges Connections.....	34
Figure 25. RSSI page .....	35
Figure 26. 2.4GHz radio basic setting page .....	36
Figure 27. 2.4GHz wireless mode page .....	37
Figure 28. QoS parameters.....	40
Figure 29. Line-of-Sight (LOS) .....	43
Figure 30. Antenna height .....	45

# Manual Conventions

<b>Bold</b>	Bold type within paragraph text indicates commands, files names, directory names, paths, output, or returned values.
<i>Italic</i>	Within commands, italics indicate a variable that the user must specify. Titles of manuals or other published documents are also set in italics.
Courier	The courier font indicates output or display.
[]	Within commands, items enclosed in square brackets are optional parameters or values that the user can choose to specify or omit.
{ }	Within commands, item enclosed in braces are options from which the user must choose.
	Within commands, the vertical bar separates options.
...	An ellipsis indicates a repetition of preceding parameter.
>	The right angle bracket separates successive menu selection.

**NOTE:** This message denotes neutral or positive information that calls out important points to the text. A note provides information that applies only in special cases.



**Caution:** Cautions call special attention to hazards that can cause system damage or data corruption, to a lesser degree than warnings.



**Warnings:** Warnings call special attention to hazards that can cause system damage, data corruption, personal injury, or death.

## Disclaimer

MIMO 2x2 Wireless Outdoor Access Point System User Manual

### Printed in the Taiwan

The instructions in this manual have been carefully checked for accuracy and are presumed to be reliable. The accuracy and adequacy of this document are the responsibilities of our company. Please, give us any comments or corrections to us.

# 1. MIMO 2x2 Wireless Outdoor Access Point System Hardware Feature

## 1.1 Hardware Outline

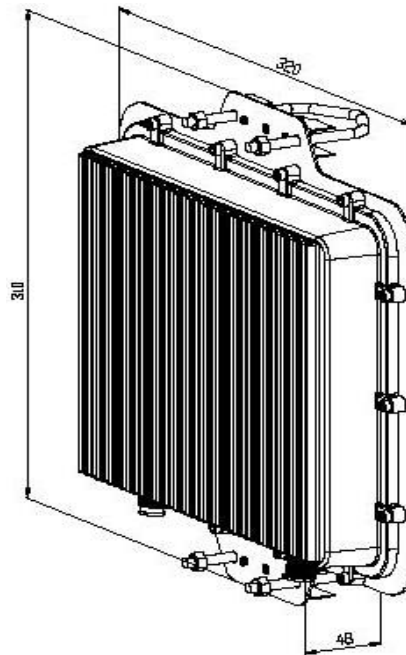


Figure 1.Outdoor unit Hardware Outline

## Product Features

- **Range** — the outdoor unit has been refined and optimized for long range application, up to 35Km.
- **Temperature** — the outdoor unit is tested for normal operation in the ambient temperatures from -35°C to 70°C. Operating in temperatures outside of this range may cause the unit malfunctioned.
- **Wind Velocity**— the outdoor unit can operate in winds up to 90mph and survive higher wind speeds up to 125mph. You must consider the known maximum wind velocity and direction at the site and be sure that any supporting structure, such as a pole, mast, or tower, built to withstand this force.
- **Lightning** — the outdoor unit includes lightning protection circuits inside. However, you should make sure that the unit, any supporting structure, and cables are all properly grounded. Additional protection using lightning rods, lightning arrestors, or surge suppressors may also employed.
- **Rain** — the weather plays one of major matters to the antenna performance for the wireless communication. The raining day, the lightning day, the cloudy day, or the windy day will make a quite big impact to both side antennas over the communication results. It will also affect the communication quality. The outdoor unit is a weatherproofed outdoor unit, which can operate in extremely weather environment. You may need to use the sealing tape around the external antenna port connectors for extra protection. If moisture enters the connector, it may cause degradation in performance or even a complete failure of the link.



## Feature Highlight

5GHz 802.11a/n based Point-to-Point Bridge

5GHz 802.11a/n based Point-to-Multipoint Bridge (up to 8 links)

2.4GHz 802.11b/g/n based high capacity access point coverage

- **Release 3.1 highlight**

- SNMP support

- Management VLAN

- NTP

- 802.1x Enterprise RADIUS support per WPA encryption

## 1.2 Interface

### 1.2.1 External Antenna Connection

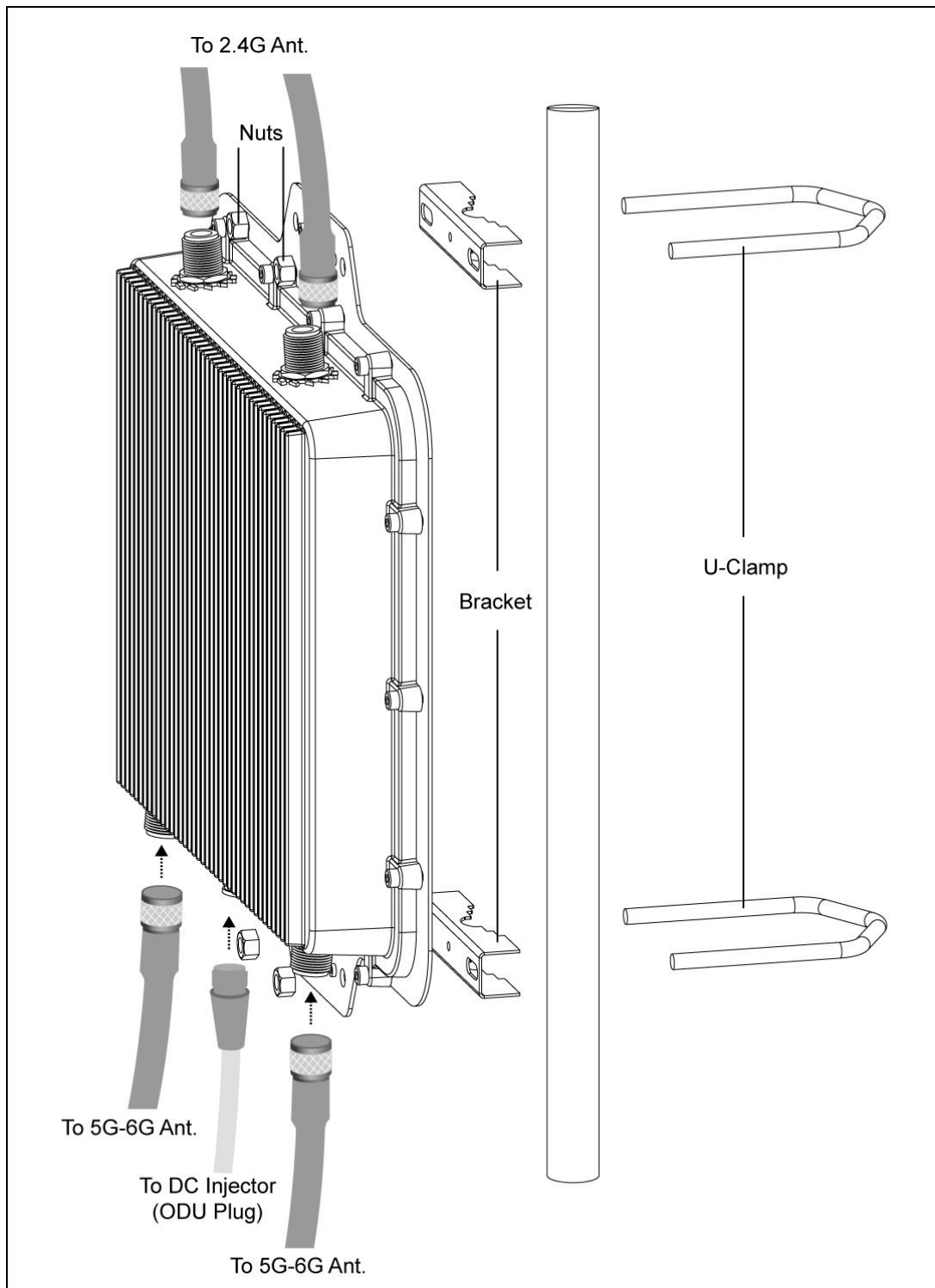


Figure 2. Antenna connection& bracket kit

### 1.2.2 Power over Ethernet (PoE) & Cable Connection

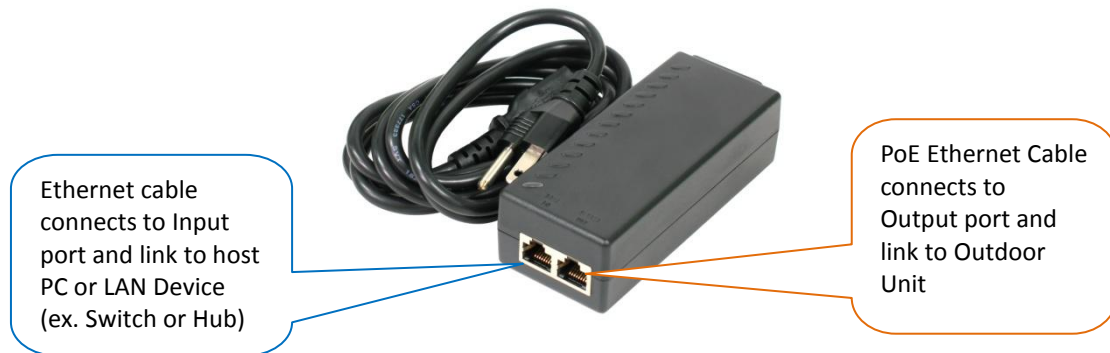


Figure 3. PoE connection

### 1.2.3 Grounding

- 1) Proper grounding is always recommended for the safety consideration.

## 1.3 Product Warranty

This product warranted against defects in materials and workmanship for a period of one year from the date of shipment. If the customer wants to have or extend longer warranty period, please contact the sales for extended warranty. During the warranty period, the defective product will be repaired or to be replaced.

## 1.4 Warranty Limitation

The foregoing warranty shall not apply to defects resulting from improper or inadequate maintenance by buyers, buyer-supplied software, interfacing, unauthorized modification, inappropriately use, operation out of the product environment specifications, or improper site preparation and maintenance.

## 1.5 System Requirement

- Windows 2000, XP, Vista Home Basic or Windows 7
- Microsoft Internet Explorer 5.5 or above versions and Google Chrome

## 1.6 Feature Summary

- Provide the Ethernet to Wireless LAN Bridge, or the Ethernet to Wireless LAN Access Point, fully IEEE 802.3 compatible Ethernet interface

- Support 10/100 Base-T Ethernet interface
- The operating mode is IEEE 802.11a/n & 802.11b/g/n infrastructure for the outdoor unit
- The dynamic data rate switching among the standards of 802.11a, 802.11b, 802.11g, 802.11n HT 20, and 802.11n HT40- and 802.11n HT 40+ are provided by **Atheros** chipset. The auto fallback feature of data rate capability optimizes the reliability, throughput and transmission range
- Using Web UI to upgrade the firmware

## 2. Getting Started

### 2.1 Setup Local Area Connection on your PC

#### 2.1.1 Start Network Configuration on your PC

- 1) Click **Start > All Programs > Accessories > Communications > Network Connections**

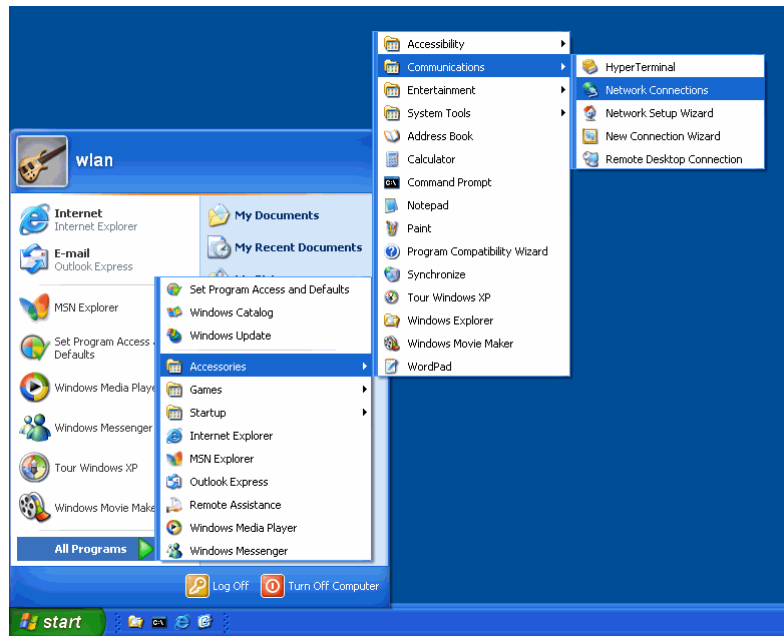


Figure 4. Windows Start Menu

- 2) Right click on the **Local Area Connection** and select **Properties**

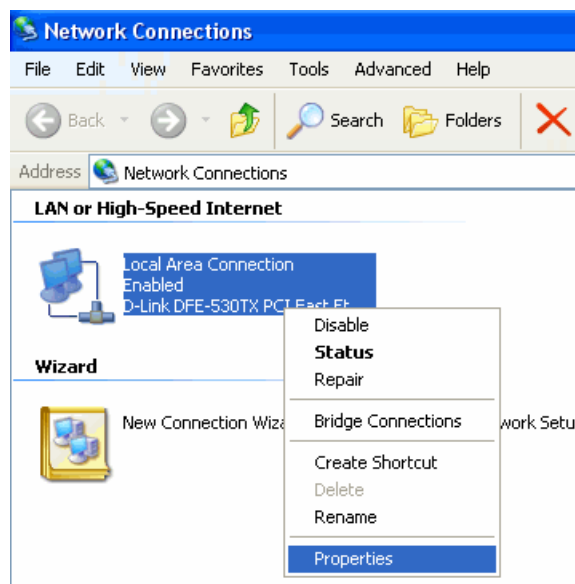


Figure 5. Network Connections

- 3) The following window shows up

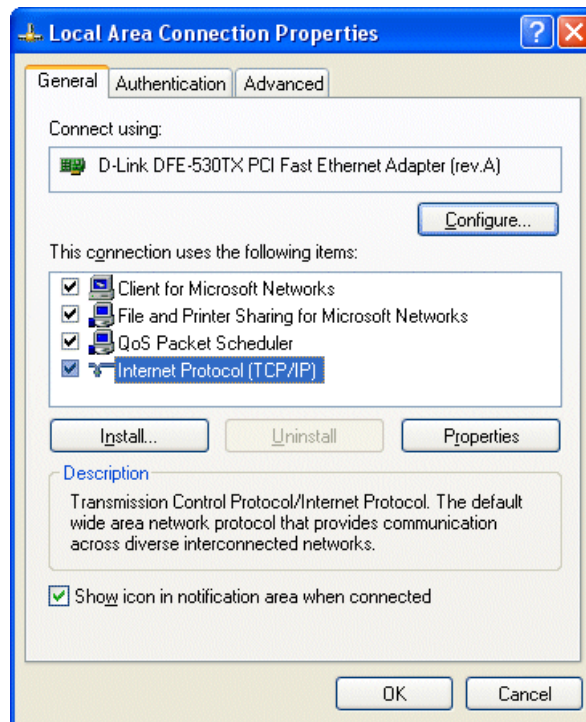


Figure 6. Local Area Connection Properties

- 4) Click **Internet Protocol (TCP/IP)** and then **Properties** (or double click on **Internet Protocol (TCP/IP)**)
- 5) Enter an **IP address** (ex. 192.168.100.2) under the same subnet as the Default IP Address of outdoor unit (**192.168.100.20**)
- 6) Enter **255.255.255.0** as Subnet Mask
- 7) Keep the **Default Gateway** and **DNS Server Address** as blank
- 8) Click **OK** when you finish above settings

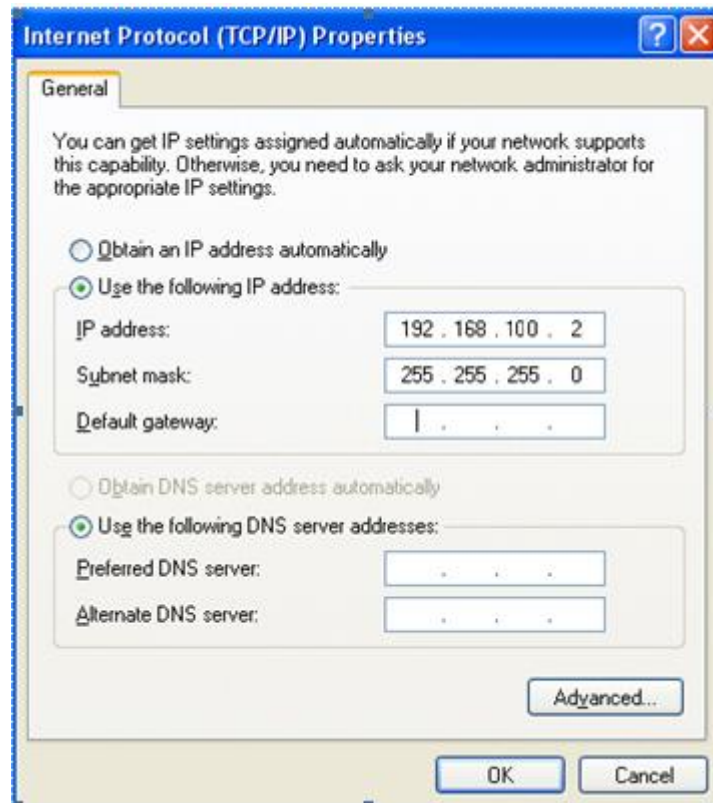


Figure 7. Internet Protocol Properties

## 2.2 Check access to the unit

Use **Ping** utility of DOS mode to check the access to the outdoor unit.

- 1) Go to **DOS** mode
- 2) Enter the command:

**ping 192.168.100.20**

The outdoor unit shall respond your ping request.



Note that use the same PC to ping different outdoor units may cause ping failure. This is because the all of the outdoor units share the same default IP address but different MAC addresses. To prevent from ping failure, you need type command **arp -d** to clear ARP table on PC before each ping.

```

Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\970601>ping 192.168.100.20

Pinging 192.168.100.20 with 32 bytes of data:

Reply from 192.168.100.20: bytes=32 time<1ms TTL=64
Reply from 192.168.100.20: bytes=32 time<1ms TTL=64
Reply from 192.168.100.20: bytes=32 time<1ms TTL=64
Reply from 192.168.100.20: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.100.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\970601>

```

Figure 8. Ping&amp; ARP command

## 2.3 Access to web pages

- 1) Launch a Web Browser
- 2) Enter the default IP address as URL (default IP address: **192.168.100.20**) and the initial home page (login page) will appear
- 3) Enter user name (default username: **Admin**) and password (default password: **Wireless**)



Note: You need to use the default user name and password when you log in for the first time.

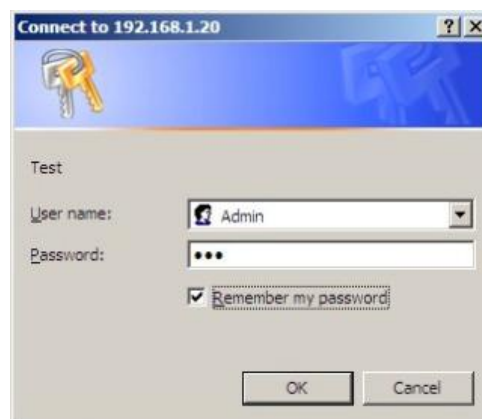


Figure 9. User Name and Password Page

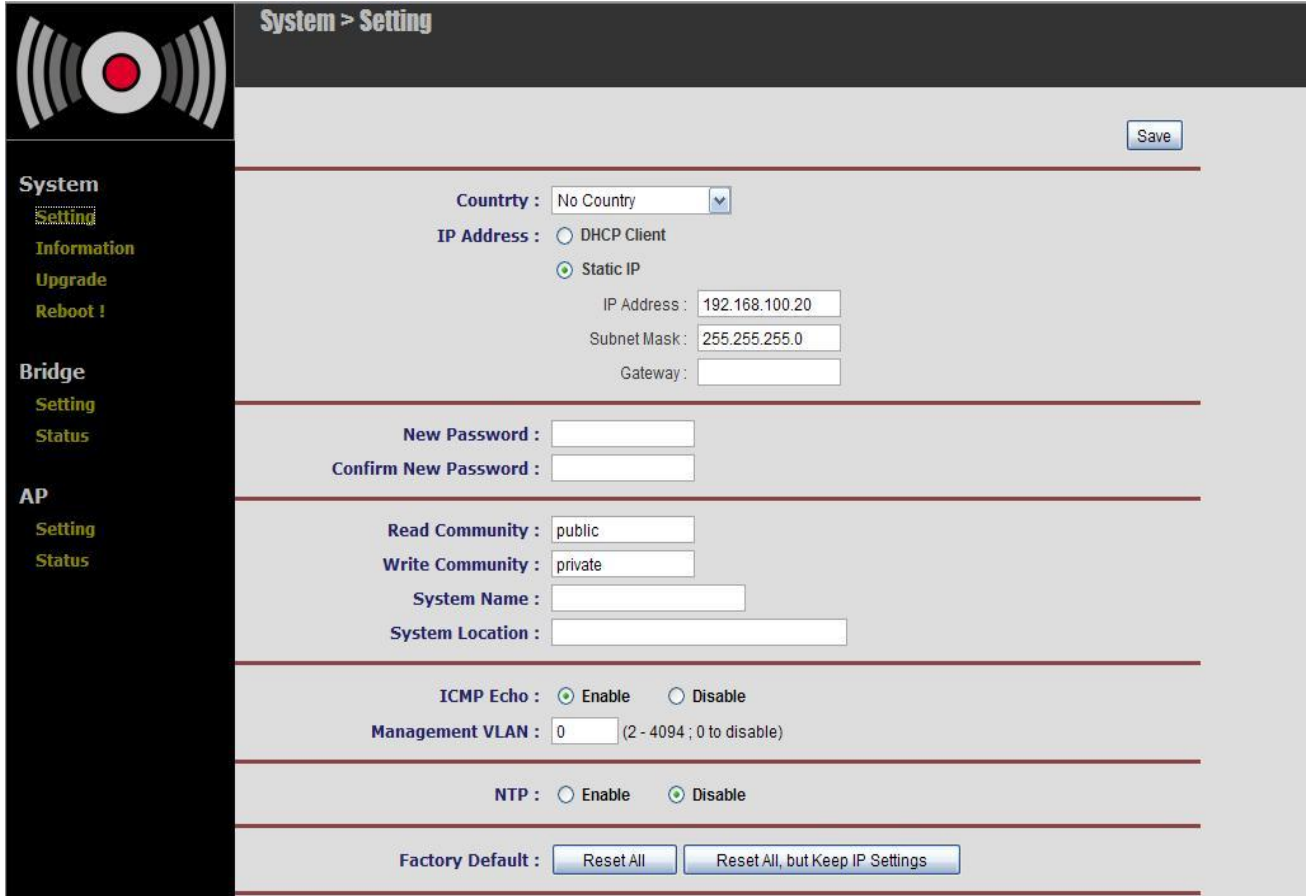
- 4) The **System Setting** page will come up after you log in successfully



## 2.4 Basic Configuration

### 2.4.1 System Setting

This page can be accessed by clicking **System > Setting**.



**System > Setting**

**System**

- Setting
- Information
- Upgrade
- Reboot !

**Bridge**

- Setting
- Status

**AP**

- Setting
- Status

**Country :** No Country

**IP Address :** ☐ DHCP Client ☒ Static IP

IP Address : 192.168.100.20

Subnet Mask : 255.255.255.0

Gateway :

**New Password :**

**Confirm New Password :**

**Read Community :** public

**Write Community :** private

**System Name :**

**System Location :**

**ICMP Echo :** ☒ Enable ☐ Disable

**Management VLAN :** 0 (2 - 4094 ; 0 to disable)

**NTP :** ☐ Enable ☒ Disable

**Factory Default :**

Figure 10. System Setting page

#### 1) Country

You can set the AP to follow different country and region regulation.

#### 2) IP Address

##### DHCP Client

Select this if your Internet Service Provider (ISP) uses a DHCP service to assign an IP address to your router when connecting to the Internet.

##### Static/ Subnet Mask/ Gateway

Note that each outdoor unit in the same network must be assigned with an unique IP address.

Therefore, you may need to have a network plan before deployment. Enter the IP address, Subnet Mask according to the plan. Changes of IP Address / Subnet Mask will be applied after you click **Save**.

### 3) Password

Change **Password** by entering a new password twice, click **Save** and then **Reboot**. User will be asked to login again with new password after reboot (the password is case sensitive).

### 4) SNMP Community

S SNMP Community name is a string for administrator to read and write the SNMP MIB from external SNMP manager. The default SNMP community name is “public” for read community, and “private” for write community. You may change the community name as your plan. Confirm your setup then clicking “**Save**” button to perform.

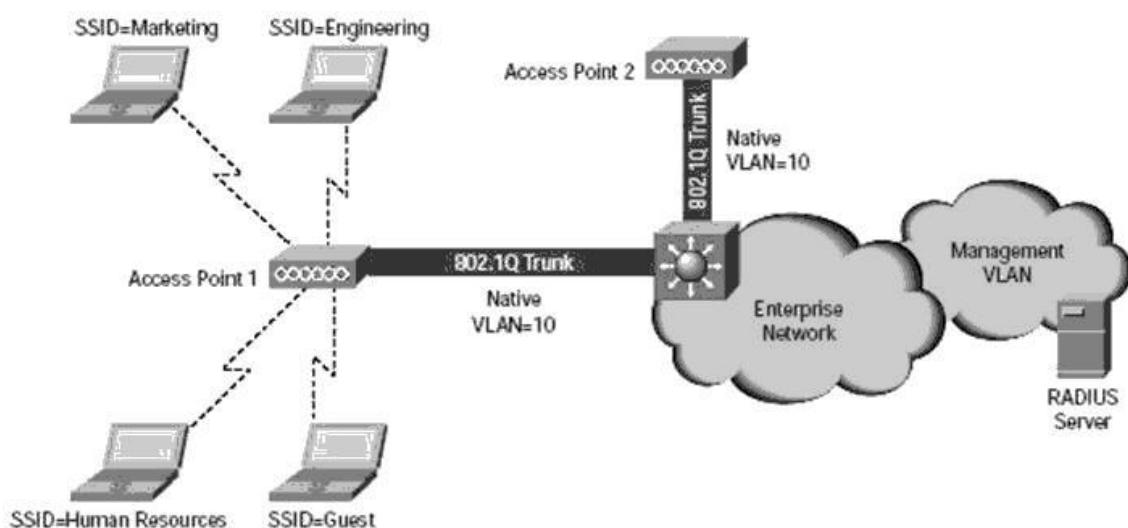
### 5) ICMP Echo

By default, the value is **Enable**. **Ping** is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer. The name comes from active sonar terminology.

Ping operates by sending Internet Control Message Protocol (ICMP) **echo request** packets to the target host and waiting for an ICMP response. In the process, it measures the time from transmission to reception round-trip time and records any packet loss. The results of the test are printed in the form of a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times, and sometimes the standard deviation of the mean.

### 6) Management VLAN

By default, the values **0** indicates **Disable**. If you have enabled VLAN tagging on your network, specify the VLAN tag ID from 2 to 4094. You can assign an SSID to a VLAN. Client devices using the SSID are grouped in that VLAN



## 7) NTP

The Network Time Protocol (NTP) is a protocol and software implementation for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. The available NTP server IP & its availability can be found by the following hyperlink (<http://www.pool.ntp.org/en/>). Enable this feature and specify the IP address of NTP server IP to get the system date & time through NTP protocol.

Time zone: specify the time zone that the product located. This setting is based on the GMT (Greenwich Mean Time).

Daylight Saving Time: Many countries, and sometimes just certain regions of countries, adopt daylight saving time (DST) during part of the year. It needs to enable or disable based on the product located countries or area.

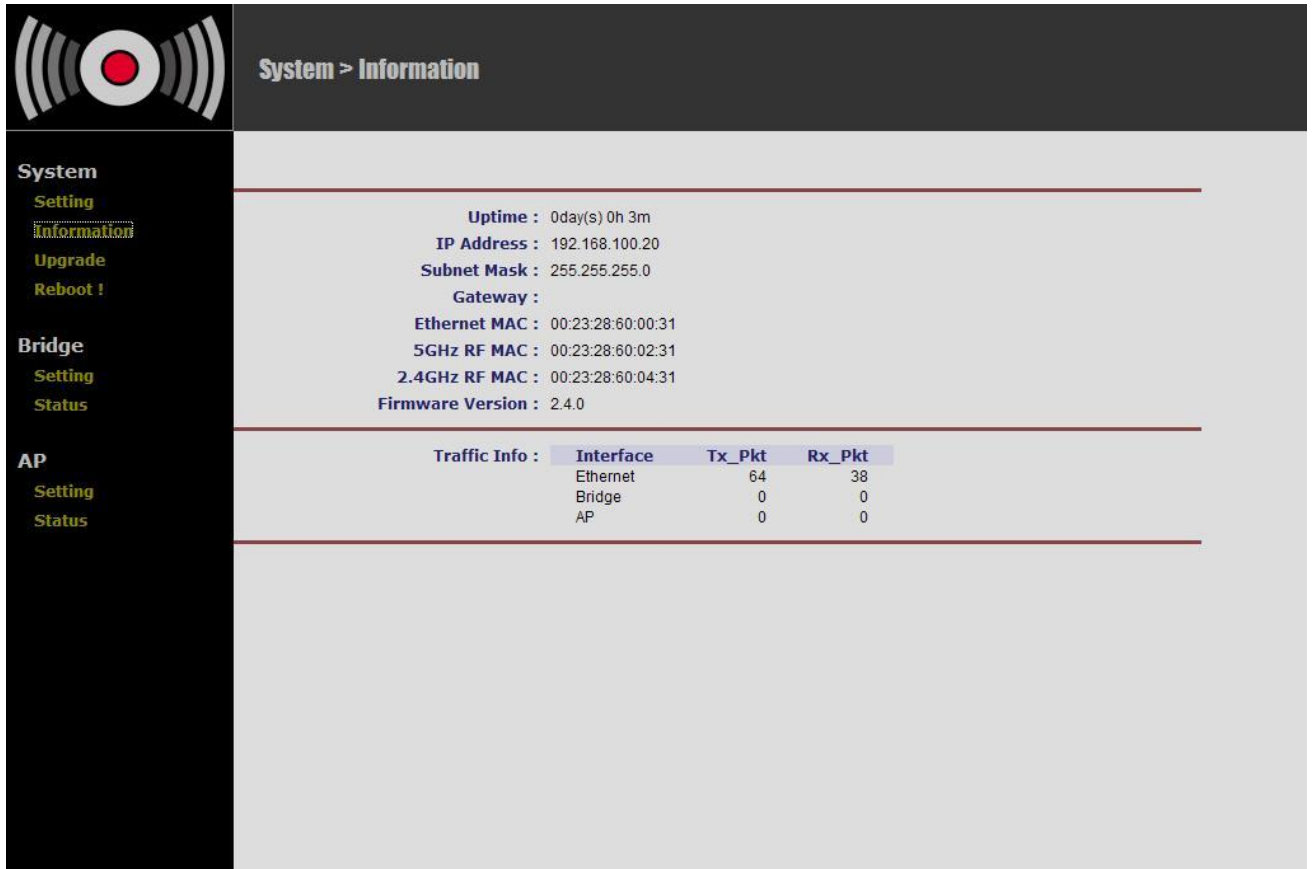
Confirm your setup then clicking **"Save"** button to perform

## 8) Factory Default

**Reset All** indicates all the settings will return to default value. **Reset All, but Keep IP Settings** indicates the IP setting stays and other setting return to default.

## 2.4.2 System Information

This page can be accessed by clicking **System > Information**.



The screenshot displays the 'System > Information' page. On the left is a dark sidebar with navigation links: System (Setting, Information, Upgrade, Reboot!), Bridge (Setting, Status), and AP (Setting, Status). The main content area has a dark header with the title 'System > Information' and a red antenna icon. Below the header, system information is listed: Uptime (0day(s) 0h 3m), IP Address (192.168.100.20), Subnet Mask (255.255.255.0), Gateway, Ethernet MAC (00:23:28:60:00:31), 5GHz RF MAC (00:23:28:60:02:31), 2.4GHz RF MAC (00:23:28:60:04:31), and Firmware Version (2.4.0). A 'Traffic Info' table shows packet counts for Ethernet, Bridge, and AP interfaces.

Interface	Tx_Pkt	Rx_Pkt
Ethernet	64	38
Bridge	0	0
AP	0	0

Figure 11. System Information page

This page lists the important system information and software / hardware inventory data.

1) **Uptime**

The elapse time since outdoor unit powered up.

2) **IP address / Subnet Mask / Gateway**

The IP address / Subnet Mask / Gateway of the wireless ODU setting.

3) **Ethernet, 5GHz & 2.4GHz RF MAC**

The MAC address of Ethernet and wireless interface.

4) **Firmware Version**

The current firmware version running on outdoor unit.

5) **Traffic Info**

The statistic data for the packets transmitted by Ethernet and the wireless interfaces.

### 2.4.3 Upgrade

The reboot function can be apply by clicking "**System -> Upgrade**" from left side menu

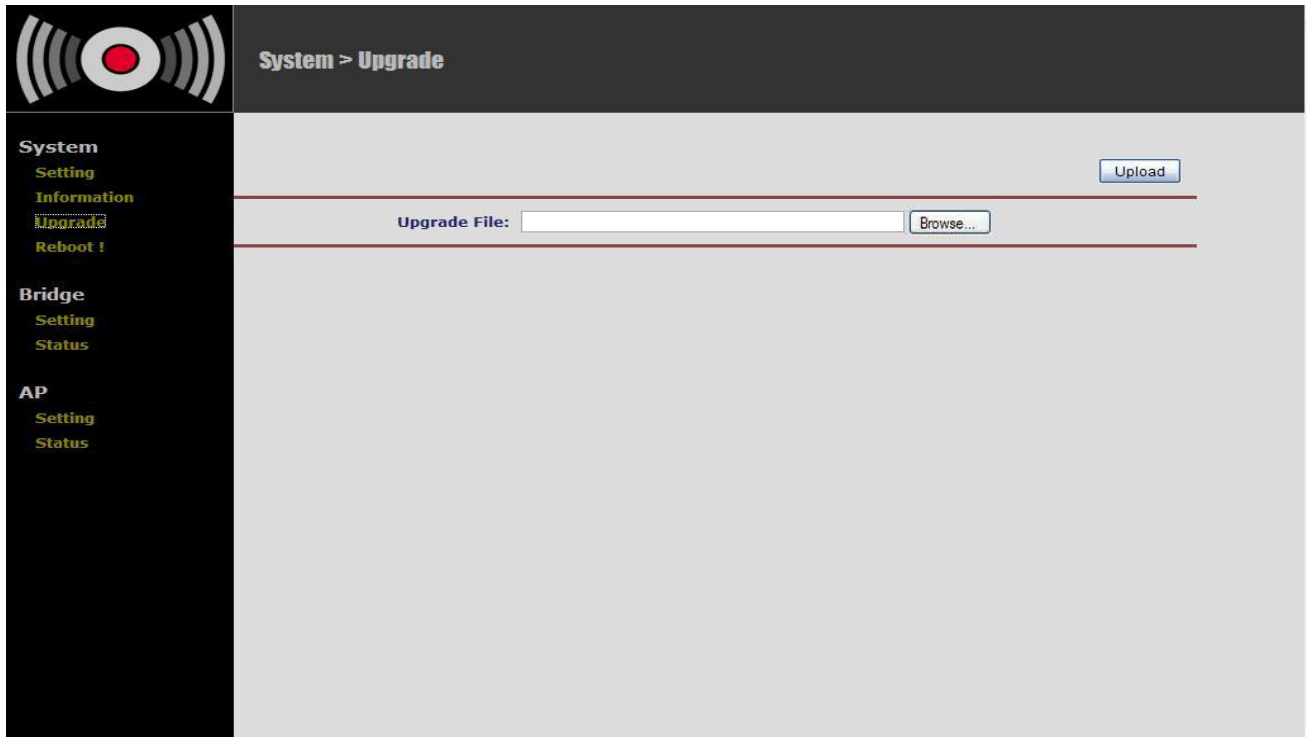


Figure 12. Upgrade page

When the new version of firmware has been received, you can upload the file by the web interface for upgrade the firmware. The page can be access by clicking "**System -> Upgrade**" from the left side menu.



**Note:**

- (a). Before upload the new version of firmware, please read the new firmware release note to confirm the new firmware features, upgrade environment, and procedures can meet the upgrade requirements.
  - (b). in case network disruption happens during file uploading, system will still keep on running with current active firmware. You may perform the file upload again when network is back to normal.
- 1) Click "Browse" button and select the firmware files to be uploaded from the PC.
  - 2) Click "Upload".
  - 3) When uploading is completed, system will prompt the successful message! Then reboot to perform the new version of firmware.
  - 4) Click "**Reboot**" for new firmware to take effect.

## 2.4.4 Reboot

You can access reboot function by clicking **System > Reboot!**.

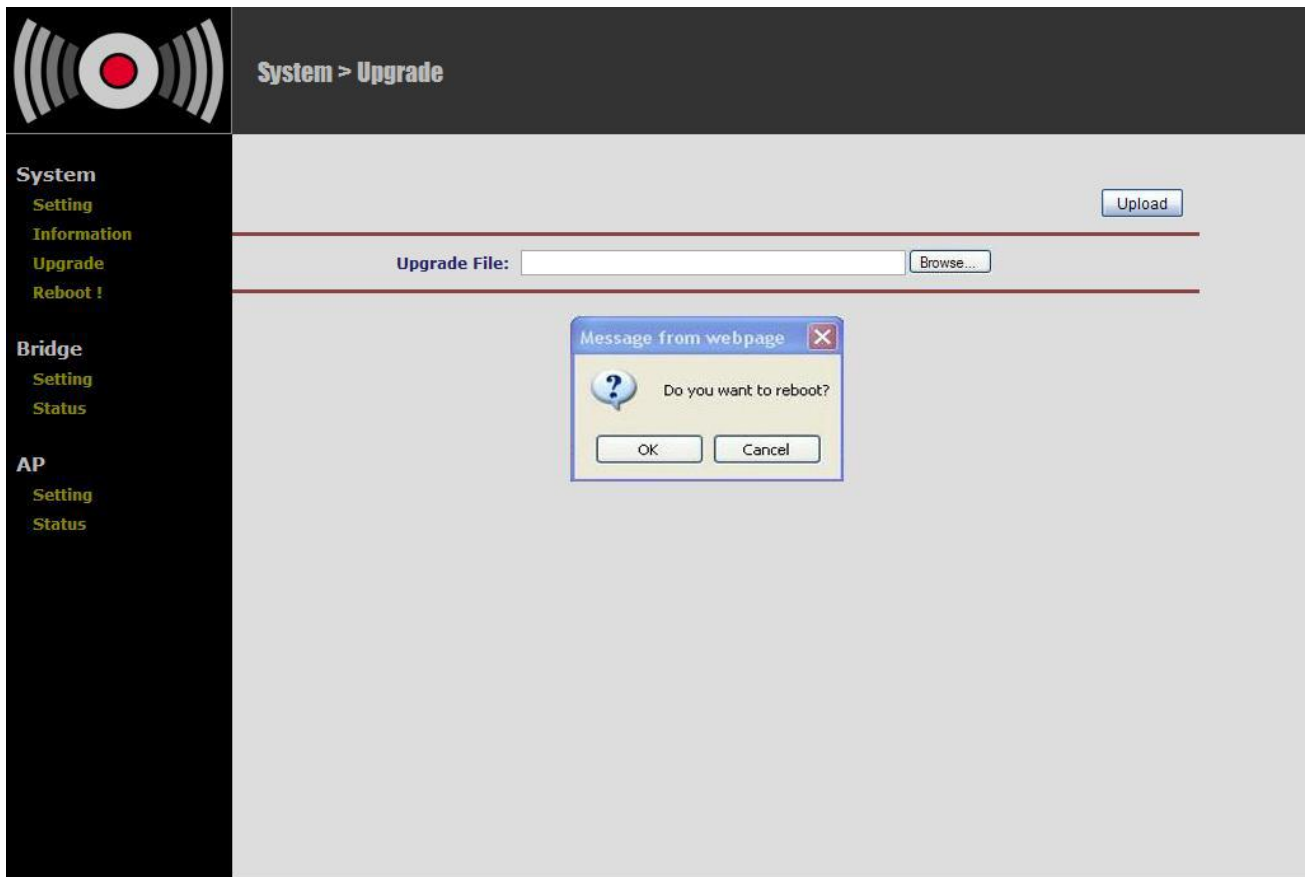


Figure 13. Reboot page

When starting reboot, system will prompt you a rebooting window. It takes at least 25 seconds to finish the reboot process.

### 3. Configure 5GHz Bridge

#### 3.1 Bridge Configuration

This page can be accessed by clicking **Bridge > Setting**.

**Bridge > Setting**

**System**  
 Setting  
 Information  
 Upgrade  
 Reboot !

**Bridge**  
 Setting  
 Status

**AP**  
 Setting  
 Status

**Save**

RF: ☒ Enable ☐ Disable

Mode: WiFi 11na HT20

Channel: 5745Mhz (Channel 149)

Rate: AUTO

Bridge Mode: ☒ Slave ☐ Master 1: 00:23:28:60:02:13

Security: ☒ No Security  
☐ WEP  
☐ WPA

Distance (Km): 1 (1 - 35)

RTS Threshold: 2347 (256 - 2347)

Tx Power: Full

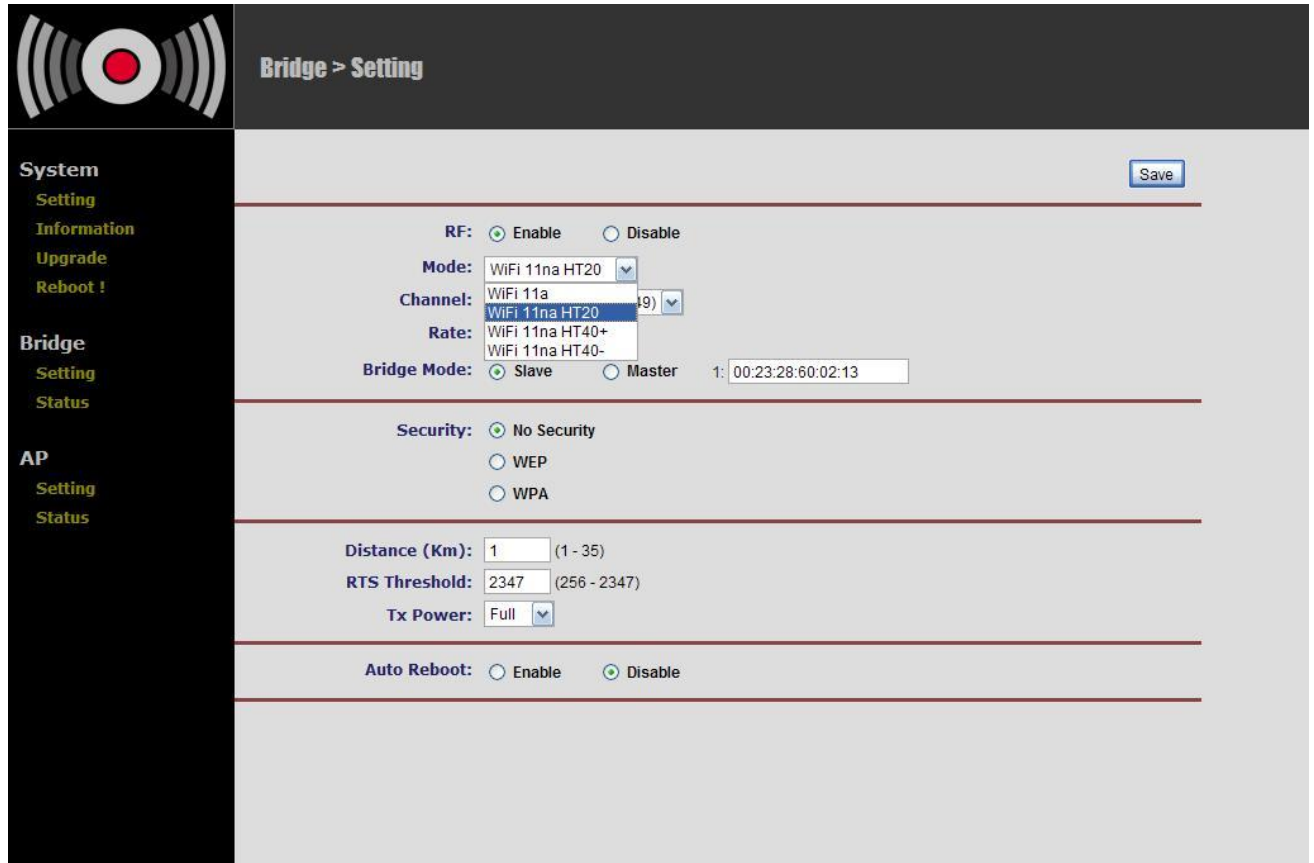
Auto Reboot: ☐ Enable ☒ Disable

Figure 14. 5GHz radio basic setting page

## 1) Enable / Disable 5GHz Radio

Click the radio box to enable/disable 5GHz Radio. It is enabled by default.

## 2) Wireless Mode



The screenshot shows the 'Bridge > Setting' page. On the left is a navigation menu with 'System' (Setting, Information, Upgrade, Reboot!), 'Bridge' (Setting, Status), and 'AP' (Setting, Status). The main content area has a 'Save' button at the top right. The settings are as follows:

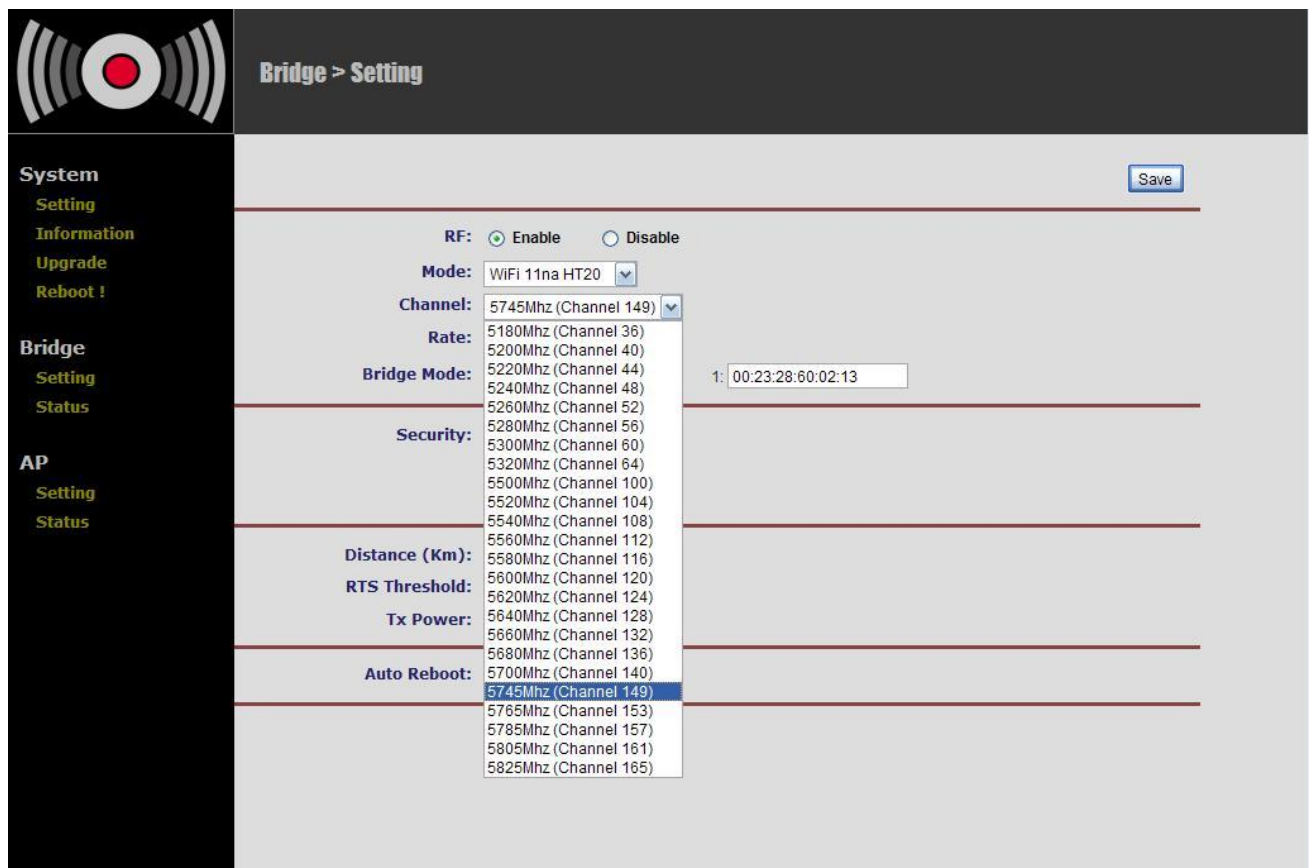
- RF:** ☒ Enable ☐ Disable
- Mode:** WiFi 11na HT20 (dropdown menu)
- Channel:** WiFi 11a (dropdown menu)
- Rate:** WiFi 11na HT20 (dropdown menu)
- Bridge Mode:** ☒ Slave ☐ Master
- Security:** ☒ No Security ☐ WEP ☐ WPA
- Distance (Km):** 1 (range 1 - 35)
- RTS Threshold:** 2347 (range 256 - 2347)
- Tx Power:** Full (dropdown menu)
- Auto Reboot:** ☐ Enable ☒ Disable

Figure 15. Wireless mode page

There are four wireless modes: **WiFi 11a** (54Mbps), **WiFi 11na HT20** (150Mbps), **WiFi 11na HT40+** and **WiFi 11na HT40-** (300Mbps). It is required to set up the same wireless mode between the bridge links to communicate with each other.



### 3) Channel (Radio Frequency)



The screenshot shows the 'Bridge > Setting' page in a web interface. The left sidebar contains navigation links for System, Bridge, and AP. The main content area is titled 'Bridge > Setting' and includes a 'Save' button. The 'RF' section has 'Enable' selected. The 'Mode' is set to 'WiFi 11na HT20'. The 'Channel' dropdown menu is open, showing a list of channels from 5180Mhz to 5825Mhz. The 'Bridge Mode' section shows a MAC address '1: 00:23:28:60:02:13'. The 'Security' section is empty. The 'Distance (Km)' section is empty. The 'RTS Threshold' section is empty. The 'Tx Power' section is empty. The 'Auto Reboot' section is empty.

**System**  
 Setting  
 Information  
 Upgrade  
 Reboot !

**Bridge**  
 Setting  
 Status

**AP**  
 Setting  
 Status

**Bridge > Setting**

Save

RF: ☒ Enable ☐ Disable

Mode: WiFi 11na HT20

Channel: 5745Mhz (Channel 149)

Rate: 5180Mhz (Channel 36)  
 5200Mhz (Channel 40)  
 5220Mhz (Channel 44)  
 5240Mhz (Channel 48)  
 5260Mhz (Channel 52)  
 5280Mhz (Channel 56)  
 5300Mhz (Channel 60)  
 5320Mhz (Channel 64)  
 5500Mhz (Channel 100)  
 5520Mhz (Channel 104)  
 5540Mhz (Channel 108)  
 5560Mhz (Channel 112)  
 5580Mhz (Channel 116)  
 5600Mhz (Channel 120)  
 5620Mhz (Channel 124)  
 5640Mhz (Channel 128)  
 5660Mhz (Channel 132)  
 5680Mhz (Channel 136)  
 5700Mhz (Channel 140)  
 5745Mhz (Channel 149)  
 5765Mhz (Channel 153)  
 5785Mhz (Channel 157)  
 5805Mhz (Channel 161)  
 5825Mhz (Channel 165)

Bridge Mode: 1: 00:23:28:60:02:13

Security:

Distance (Km):

RTS Threshold:

Tx Power:

Auto Reboot:

Figure 16. Channel page

Select a radio channel according to the availability or system plan. It is required for all Bridges on outdoor units to have the same radio frequency to communicate with each other.

## 4) Data Rate

**Bridge > Setting**

**System**  
 Setting  
 Information  
 Upgrade  
 Reboot !

**Bridge**  
 Setting  
 Status

**AP**  
 Setting  
 Status

**Save**

RF: ☒ Enable ☐ Disable

Mode: WiFi 11na HT40+

Channel: 5785Mhz (Channel 157)

Rate: AUTO

Bridge Mode: AUTO

Security:

Distance (Km):

RTS Threshold:

Tx Power:

Auto Reboot: ☒ Enable ☐ Disable

Master 1: 00:23:28:60:02:13

Rate dropdown options:  
 AUTO  
 MCS 0 (15.0M)  
 MCS 1 (30.0M)  
 MCS 2 (45.0M)  
 MCS 3 (60.0M)  
 MCS 4 (90.0M)  
 MCS 5 (120.0M)  
 MCS 6 (135.0M)  
 MCS 7 (150.0M)  
 MCS 8 (30.0M)  
 MCS 9 (60.0M)  
 MCS 10 (90.0M)  
 MCS 11 (120.0M)  
 MCS 12 (180.0M)  
 MCS 13 (240.0M)  
 MCS 14 (270.0M)  
 MCS 15 (300.0M)

Figure 17. Data Rate page

Available data rate range is dependent upon the selection of Wireless Mode setting. Rates of 6, 9, 12, 18, 24, 36, 48 and 54Mbps are supported for the wireless mode of 54Mbps (802.11a). And, rates of MCS-0, MCS-1, MCS-2, MCS-3, MCS-4, MCS-5, MCS-6, MCS-7, MCS-8, MCS-9, MCS-10, MCS-11, MCS-12, MCS-13, MCS-14, and MCS-15 are supported for the wireless mode of 802.11a/n HT-20, 802.11a/n HT-40+, and 802.11a/n HT-40-. **The default data rate is "Auto". It is recommended to keep the default data rate for bridge mode.**

## 5) Bridge Mode

**Bridge > Setting**

**System**  
 Setting  
 Information  
 Upgrade  
 Reboot !

**Bridge**  
 Setting  
 Status

**AP**  
 Setting  
 Status

**Save**

RF: ☒ Enable ☐ Disable

Mode: WiFi 11na HT40+

Channel: 5785Mhz (Channel 157)

Rate: AUTO

Bridge Mode: ☐ Slave ☒ Master

1: 00:23:28:60:02:13  
 2:  
 3:  
 4:  
 5:  
 6:  
 7:  
 8:

Security: ☒ No Security  
☐ WEP  
☐ WPA

Distance (Km): 1 (1 - 35)

RTS Threshold: 2347 (256 - 2347)

Tx Power: Full

Auto Reboot: ☐ Enable ☒ Disable

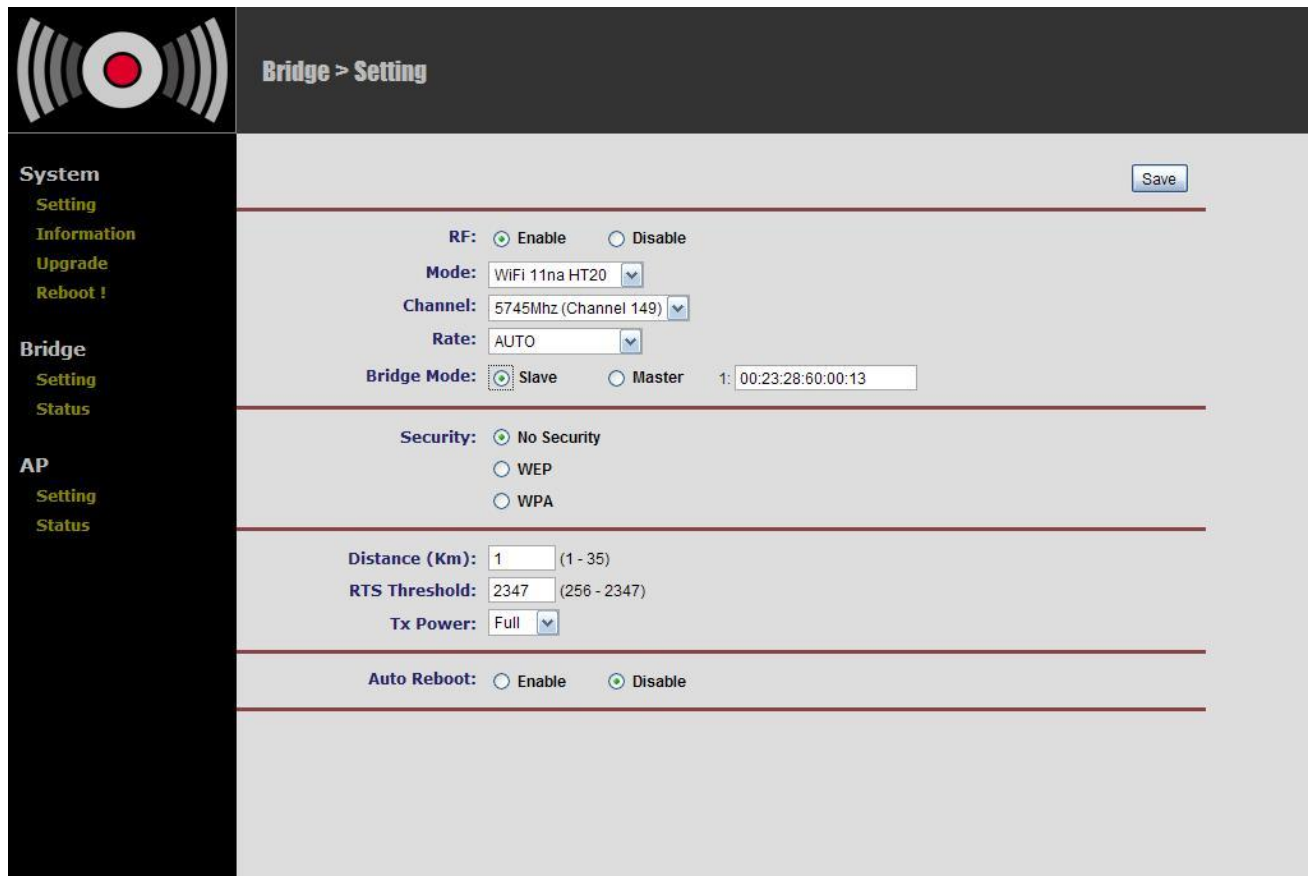
Figure 18. Bridge mode page

Select **Master** for Master Bridge mode, or select **Slave** for Slave Bridge mode. The default mode is **Slave**.



Note: When **Master** mode is enabled, the remote bridge mode shall set as **Slave** mode. One bridge network shall have only one outdoor unit in **Master** mode, and the others in **Slave** mode.

## 6) Remote Bridge Setup



**Bridge > Setting**

**System**  
 Setting  
 Information  
 Upgrade  
 Reboot !

**Bridge**  
 Setting  
 Status

**AP**  
 Setting  
 Status

**Save**

RF: ☒ Enable ☐ Disable

Mode: WiFi 11na HT20

Channel: 5745Mhz (Channel 149)

Rate: AUTO

Bridge Mode: ☒ Slave ☐ Master 1: 00:23:28:60:00:13

Security: ☒ No Security  
☐ WEP  
☐ WPA

Distance (Km): 1 (1 - 35)

RTS Threshold: 2347 (256 - 2347)

Tx Power: Full

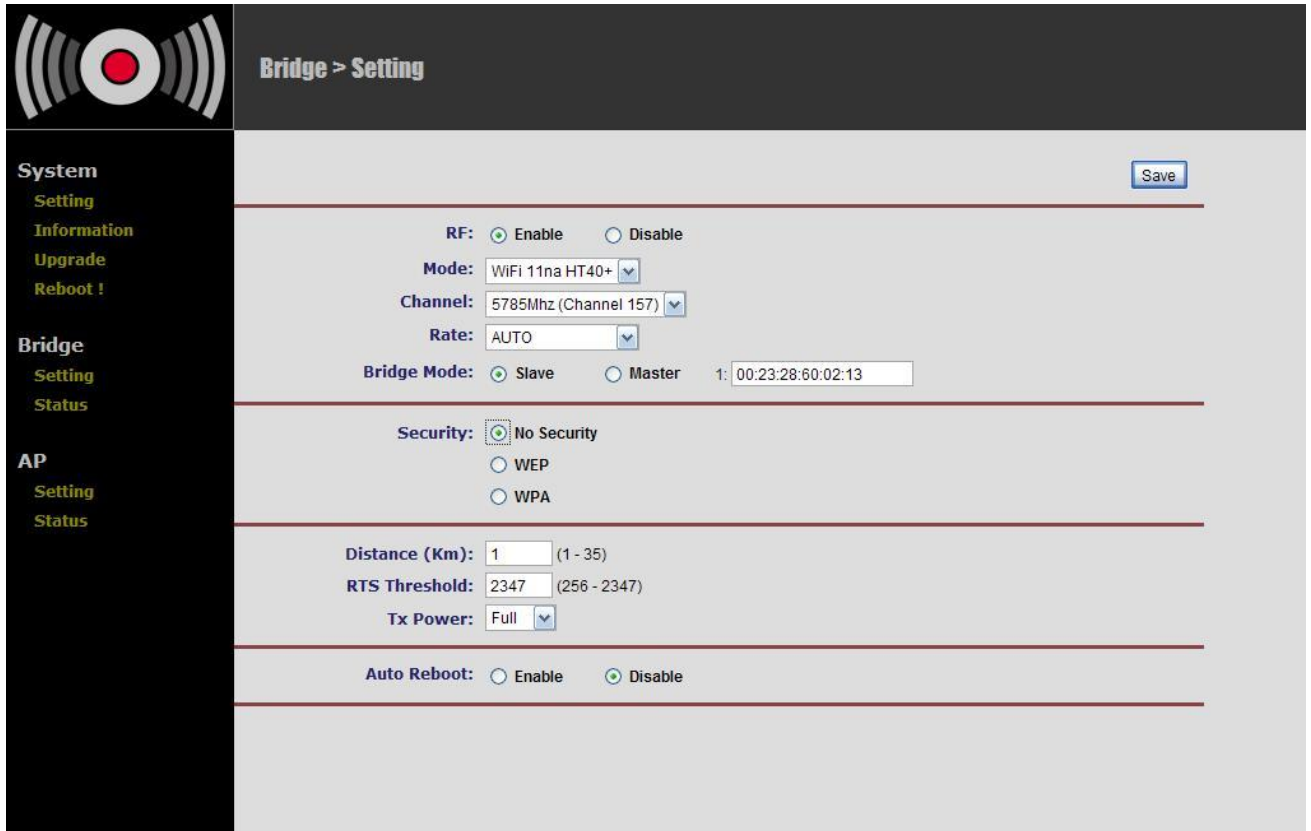
Auto Reboot: ☐ Enable ☒ Disable

Figure 19. Remote bridge setup page

In order to establish the wireless link between Bridge Radios, the MAC address of remote Bridge(s) needs to be registered in the address filed. Enter the MAC address with format as xx:xx:xx:xx:xx:xx (x is the hexadecimal digit). Master Bridge Radio may accommodate up to **8** remote MAC addresses by the current firmware. In addition, Slave Bridge Radio supports only **1** MAC address which have to be the Master Bridge.

## 7) Security

Please refer to Chapter 4. for security setting.



**Bridge > Setting**

**System**  
 Setting  
 Information  
 Upgrade  
 Reboot !

**Bridge**  
 Setting  
 Status

**AP**  
 Setting  
 Status

**RF:** ☒ Enable ☐ Disable

**Mode:** WiFi 11na HT40+ ▼

**Channel:** 5785Mhz (Channel 157) ▼

**Rate:** AUTO ▼

**Bridge Mode:** ☒ Slave ☐ Master 1: 00:23:28:60:02:13

**Security:** ☒ No Security  
☐ WEP  
☐ WPA

**Distance (Km):** 1 (1 - 35)

**RTS Threshold:** 2347 (256 - 2347)

**Tx Power:** Full ▼

**Auto Reboot:** ☐ Enable ☒ Disable

**Save**

Figure 20. Security page

## 8) Distance (Km)

Enter the distance according to the longest link between the Master and Slaves in the network. The value needs to be greater than or equal to the real distance. The range is from 1Km to 35Km.

## 9) RTS Threshold

In order to prevent the transmission collision in a hidden nodes environment, Bridge may send a RTS (Request To Send) before transmitting the data frame from remote Bridge. You may define a threshold for those frame size greater than the threshold need to activate RTS mechanism. The valid range is from 256 to 2347. Set low value to this threshold may avoid collision, but the RTS frame would consume bandwidth.



**Note:** In Point to Multi-Point application, the transmission collision may be caused by hidden nodes affection in particular environment or network configuration. Setting smaller number of RTS threshold could alleviate the hidden nodes problem.

10) **Tx Power**

Available selections of transmit power are **Full**, **-3dB**, **-6dB** and **-9dB**. Select the appropriate transmit power according to the distance and environmental factor between Bridges.

11) **Auto Reboot**

Default is **Disable**. When this function is enabled, near-end AP cannot receive **alive message** from far-end AP in a certain period. Then this function will perform automatically at near-end AP without notice. The **alive message** is communicated between near-end & far-end AP via 5GHz Bridge links.

12) To make changes take effect, click **Save** and **Reboot** when you finish all settings.

## 4. Bridge Security Setting

To have a secured data transmission, outdoor unit provides the following encryption types.

- No Security
- 64-bit & 128-bit WEP
- WPA TKIP-PSK or AES-PSK



Note that it is required to have the same security setting between Bridges to communicate.

### 4.1 Bridge Security Setting - WEP

This page can be accessed by clicking **Bridge > Setting**.

**Bridge > Setting** Save

RF: ☒ Enable ☐ Disable

Mode: WiFi 11na HT40+ ▼

Channel: 5785Mhz (Channel 157) ▼

Rate: AUTO ▼

Bridge Mode: ☒ Slave ☐ Master 1: 00:23:28:60:02:13

Security: ☐ No Security ☒ WEP

☐ Key 1

☐ Key 2

☐ Key 3

☐ Key 4

☐ WPA

Distance (Km): 1 (1 - 35)

RTS Threshold: 2347 (256 - 2347)

Tx Power: Full ▼

Auto Reboot: ☐ Enable ☒ Disable

Figure 21. Bridge security page - WEP

#### 1) Security Mode

Select **WEP** to enable the security mode.

2) **Key Entry Method**

Hexadecimal: The key must be hexadecimal (0-9, A-F).

3) **Key Length**

For **WEP** encryption, the key length can be **10 HEX**.

4) **Encryption Key**

The WEP key can be in one of the following formats: 5 characters, 10 hex digits, 13 characters, or 26 hex digits.



Note that it is required to have the same security setting between Bridges to communicate.

- 5) To make changes take effect, click **Save** and **Reboot** when you finish all settings.

## 4.2 Bridge Security Setting – WPA

This page can be accessed by clicking **Bridge > Setting**.

**Bridge > Setting**

**System**  
 Setting  
 Information  
 Upgrade  
 Reboot !

**Bridge**  
 Setting  
 Status

**AP**  
 Setting  
 Status

**Save**

RF: ☒ Enable ☐ Disable

Mode: WiFi 11na HT40+

Channel: 5785Mhz (Channel 157)

Rate: AUTO

Bridge Mode: ☒ Slave ☐ Master 1: 00:23:28:60:02:13

Security: ☐ No Security  
☐ WEP  
☒ WPA

Cypher: ☐ TKIP ☐ AES

PSK: (8 - 63 characters)

Distance (Km): 1 (1 - 35)

RTS Threshold: 2347 (256 - 2347)

Tx Power: Full

Auto Reboot: ☐ Enable ☒ Disable

Figure 22. Bridge Security page - WPA

1) **Security Mode**



Select **WPA** to enable the security mode.

2) **WPA Mode**

Select **WPA** according to the security plan.

3) **Cypher Mode**

Select **Cypher** according to the security plan. **TKIP** or **AES**.

4) **PSK**

The key is an ASCII string with length from 8 to 63 characters.

5) To make changes take effect, click **Save** and **Reboot** when you finish all settings.

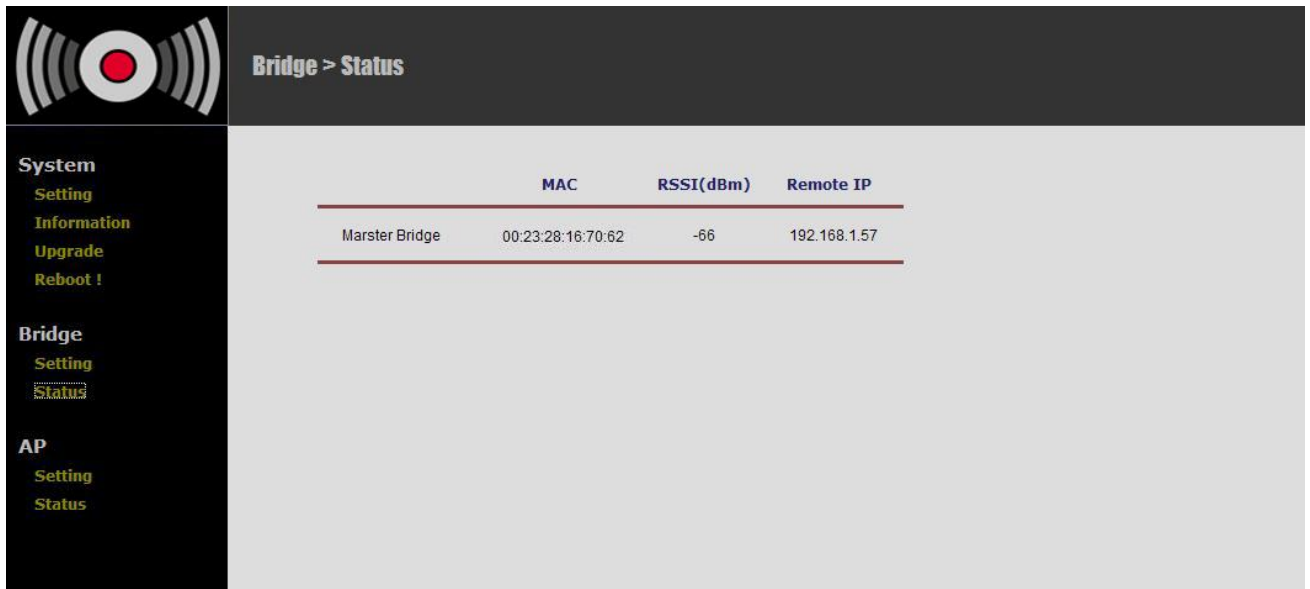


Note that it is required to have the same security setting between Bridges to communicate.

## 5. Network Management

### 5.1 5GHz Bridge Connection Status

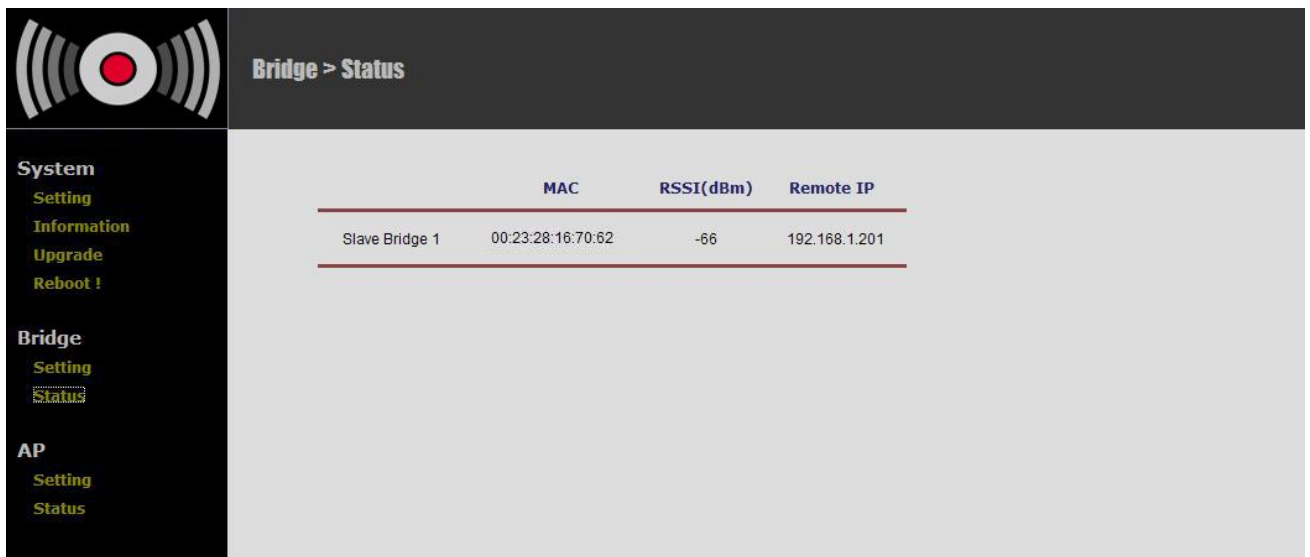
This page shows the local and remote Bridges and can be accessed by clicking **Bridge > Status**.



The screenshot shows the 'Bridge > Status' page. On the left is a navigation menu with sections: System (Setting, Information, Upgrade, Reboot!), Bridge (Setting, Status), and AP (Setting, Status). The 'Status' link under the Bridge section is highlighted. The main content area displays a table with the following data:

	MAC	RSSI(dBm)	Remote IP
Master Bridge	00:23:28:16:70:62	-66	192.168.1.57

Figure 23. Master/Slave Bridges connection status



The screenshot shows the 'Bridge > Status' page. On the left is a navigation menu with sections: System (Setting, Information, Upgrade, Reboot!), Bridge (Setting, Status), and AP (Setting, Status). The 'Status' link under the Bridge section is highlighted. The main content area displays a table with the following data:

	MAC	RSSI(dBm)	Remote IP
Slave Bridge 1	00:23:28:16:70:62	-66	192.168.1.201

Figure 24. Master/Slave Bridges Connections

#### 1) Slave Bridge

This line shows the MAC address of Slave Bridge as well as its status.

### 5.1.1 RSSI

By clicking on MAC address hyperlink of desired remote Bridge, the system will show a RSSI page for you to monitor the bridge link.



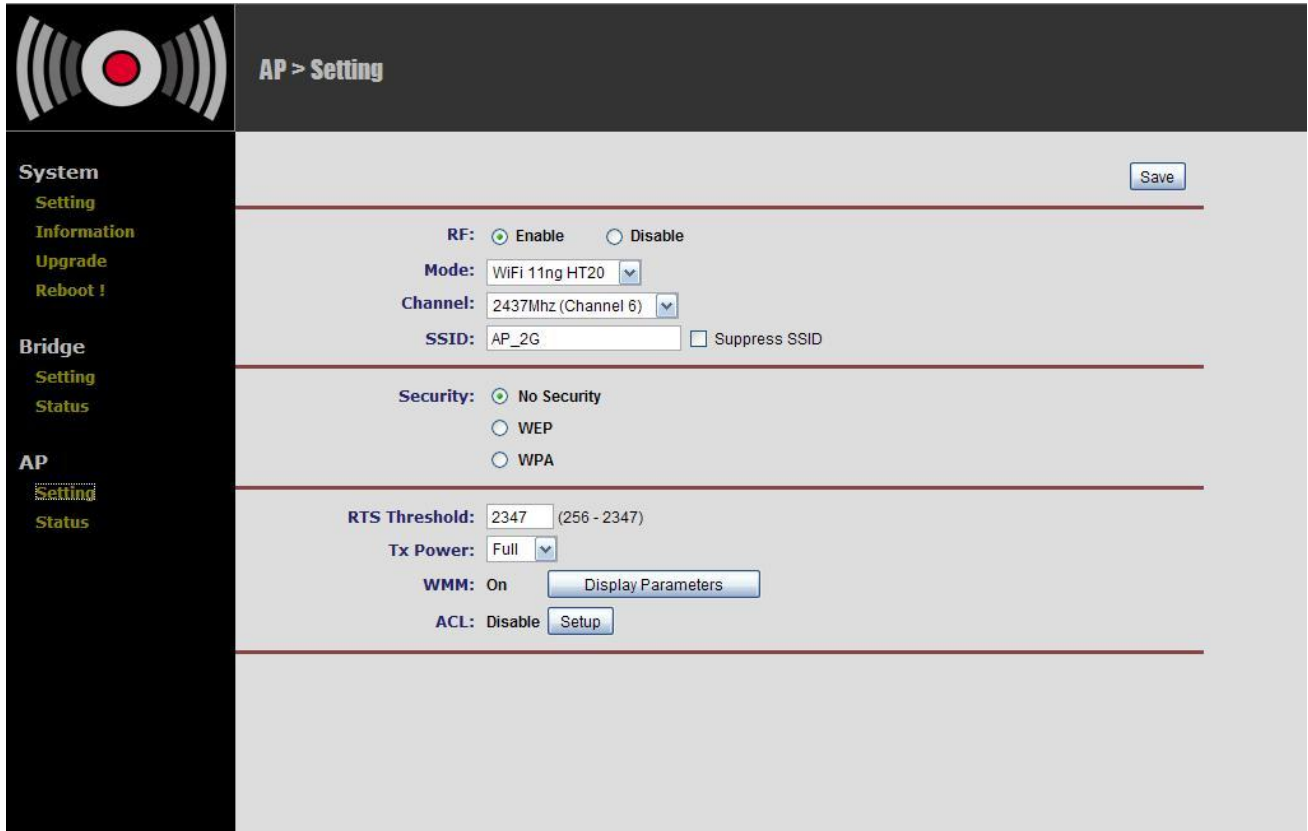
Figure 25. RSSI page

RSSI values on this page are refreshed automatically.

## 6. Configure 2.4GHz AP

### 6.1 AP Configuration

This page can be accessed by clicking **AP > Setting**.



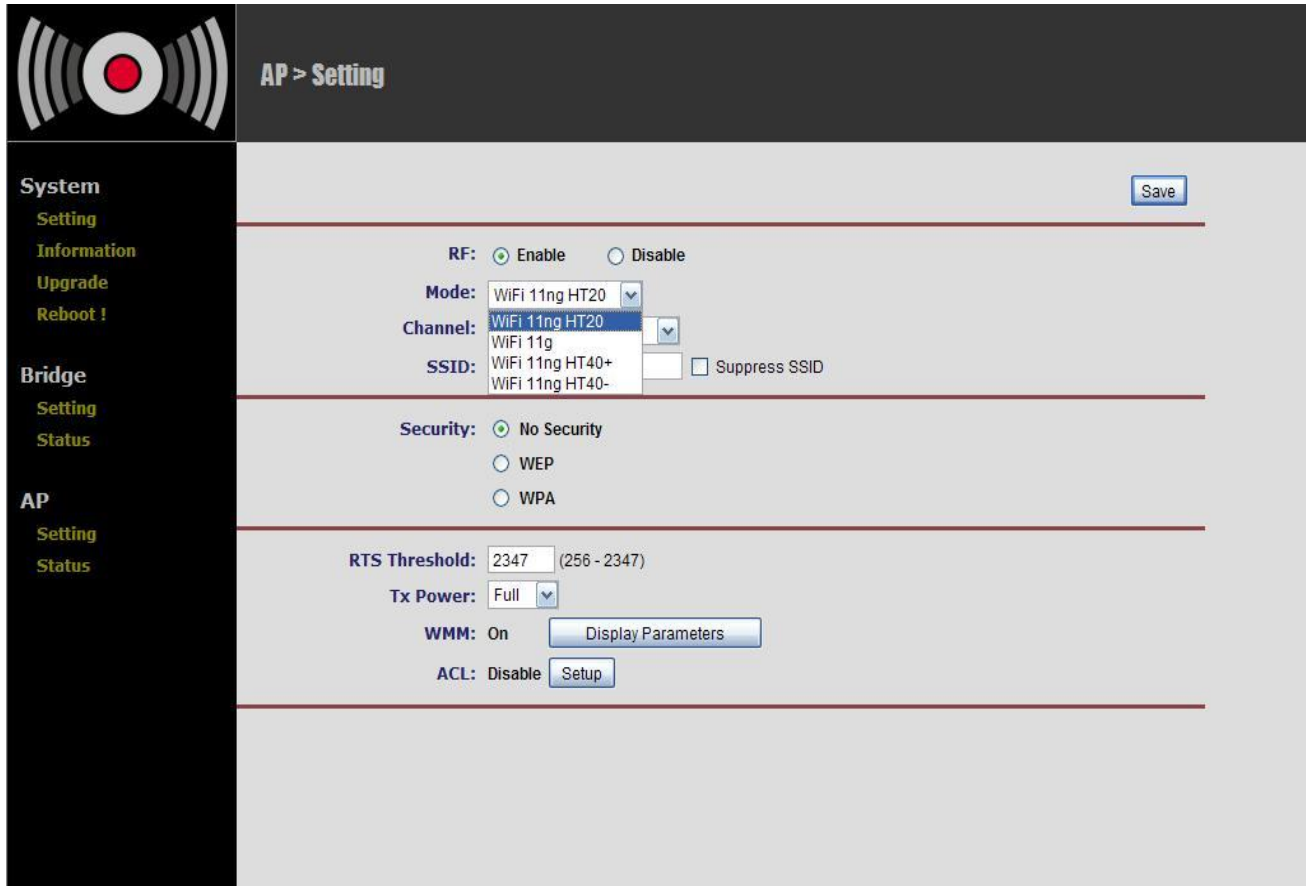
The screenshot shows the 'AP > Setting' configuration page. On the left is a dark sidebar with a wireless signal icon at the top. The sidebar contains three main sections: 'System' with links for Setting, Information, Upgrade, and Reboot!; 'Bridge' with links for Setting and Status; and 'AP' with links for Setting and Status. The 'AP > Setting' page has a light gray background with a dark header bar. The header bar contains a 'Save' button on the right and the title 'AP > Setting' on the left. The main content area is divided into sections by horizontal lines. The first section contains 'RF: Enable' (selected) and 'Disable' (radio buttons), 'Mode: WiFi 11ng HT20' (dropdown), 'Channel: 2437Mhz (Channel 6)' (dropdown), 'SSID: AP\_2G' (text input), and a 'Suppress SSID' checkbox. The second section contains 'Security: No Security' (selected), 'WEP' (radio button), and 'WPA' (radio button). The third section contains 'RTS Threshold: 2347' (text input) with '(256 - 2347)' in parentheses, 'Tx Power: Full' (dropdown), 'WMM: On' (radio button) with a 'Display Parameters' button, and 'ACL: Disable' (radio button) with a 'Setup' button.

Figure 26. 2.4GHz radio basic setting page

### 1) Enable / Disable 5GHz Radio

Click the radio box to enable/disable 2.4GHz Radio. It is enabled by default.

### 2) Wireless Mode



The screenshot shows the 'AP > Setting' page. On the left is a navigation menu with sections: System (Setting, Information, Upgrade, Reboot!), Bridge (Setting, Status), and AP (Setting, Status). The main content area is titled 'AP > Setting' and contains the following settings:

- RF:** ☒ Enable ☐ Disable
- Mode:** WiFi 11ng HT20 (dropdown menu)
- Channel:** WiFi 11ng HT20 (dropdown menu)
- SSID:** WiFi 11ng HT40+ (text input) ☐ Suppress SSID
- Security:** ☒ No Security ☐ WEP ☐ WPA
- RTS Threshold:** 2347 (256 - 2347)
- Tx Power:** Full (dropdown menu)
- WMM:** On [Display Parameters](#)
- ACL:** Disable [Setup](#)

A 'Save' button is located at the top right of the settings area.

Figure 27. 2.4GHz wireless mode page

There are four wireless modes: **WiFi 11g** (54Mbps), **WiFi 11ng HT20** (150Mbps), **WiFi 11ng HT40+** and **WiFi 11ng HT40-** (300Mbps).

### 3) Channel (Radio Frequency)

Select a radio channel according to the availability or system plan.

### 4) SSID

The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network. For added security, you should change the SSID from the default **AP\_2G** to a unique name. This

option can make the SSID invisible from site survey tool. Enable this function only if you do not want the Access Point to be found by others.

#### 5) **Suppress SSID**

When you enable “Suppress SSID” function, SSID information will be removed from AP broadcast frame. Thus, only those stations aware of the SSID can associate with AP. The default setting is disabled.

#### 6) **Security**

By default, the security is disabled (**No Security**). Refer to the next section to configure the security features such as **WEP**, **WPA**, **WPA-PSK**, **WPA2** and **WPA2-PSK**.

#### 7) **RTS Threshold**


By default, the value is **2347**. This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications are recommended.

#### 8) **Tx Power**

By default, the value is **Full**. Available selections of Transmit Power are **Full**, **-3dB**, **-6dB** and **-9dB**. Select the appropriate Transmit Power according to the distance and environmental factor between AP to client.

#### 9) **WMM**

Multimedia applications in a WiFi network require Quality of Service (QoS) functionality. The system default enabled WMM QoS feature, and it will prioritize traffic and optimizes the way shared network resources among different applications. It works well for data traffic from applications such as web browser, file transfer, or email, but it is inadequate for multimedia applications. Voice over Internet Protocol (VoIP), video streaming, and interactive gaming are highly sensitive to latency increases and throughput reductions, and required to enable QoS feature. The QoS parameters is default according to IEEE 802.11e as Figure 22.



AP > Setting > WMM Parameters

**System**

Setting

Information

Upgrade

Reboot !

**Bridge**

Setting

Status

**AP**

Setting

Status

	CWMin	CWMax	AIFS	TxOpLimit	ACM	NoAck
AC_BE	15	63	3	0	Off	Off
AC_BK	15	1023	7	0	Off	Off
AC_VI	7	15	1	3008	Off	Off
AC_VO	3	7	1	1504	Off	Off

Figure 28. QoS parameters

Note:


- AC\_BE: Best effort packet
- AC\_BK: Background packet
- AC\_VI: Video packet
- AC\_VO: Voice packet

#### 10) ACL(Access Control)

You may choose to **Disabled**, **Allow**, or **Deny**. By selecting **Allow**, only the address listed in the table will have access to the network; all other clients will be blocked. On the other hand, select **Deny**, means only the listed MAC addresses will be blocked from accessing the network; all other clients will have access to the network.

**MAC Address:** Enter the MAC address.

This table lists the blocked or allowed MAC addresses; you may delete selected MAC address or delete all the addresses from the table by clicking **Delete**.


**AP > Setting > ACL**

**System**

Setting

Information

Upgrade

Reboot !

**Bridge**

Setting

Status

**AP**


Setting

Status

**ACL Mode:** ☐ Disable ☒ Allow ☐ Deny

**MAC Address:**

1:		16:	
2:		17:	
3:		18:	
4:		19:	
5:		20:	
6:		21:	
7:		22:	
8:		23:	
9:		24:	
10:		25:	
11:		26:	
12:		27:	
13:		28:	
14:		29:	
15:		30:	


**AP > Setting > ACL**

**System**

Setting

Information

Upgrade

Reboot !

**Bridge**

Setting

Status

**AP**

Setting

Status

**ACL Mode:** ☐ Disable ☐ Allow ☒ Deny

**MAC Address:**

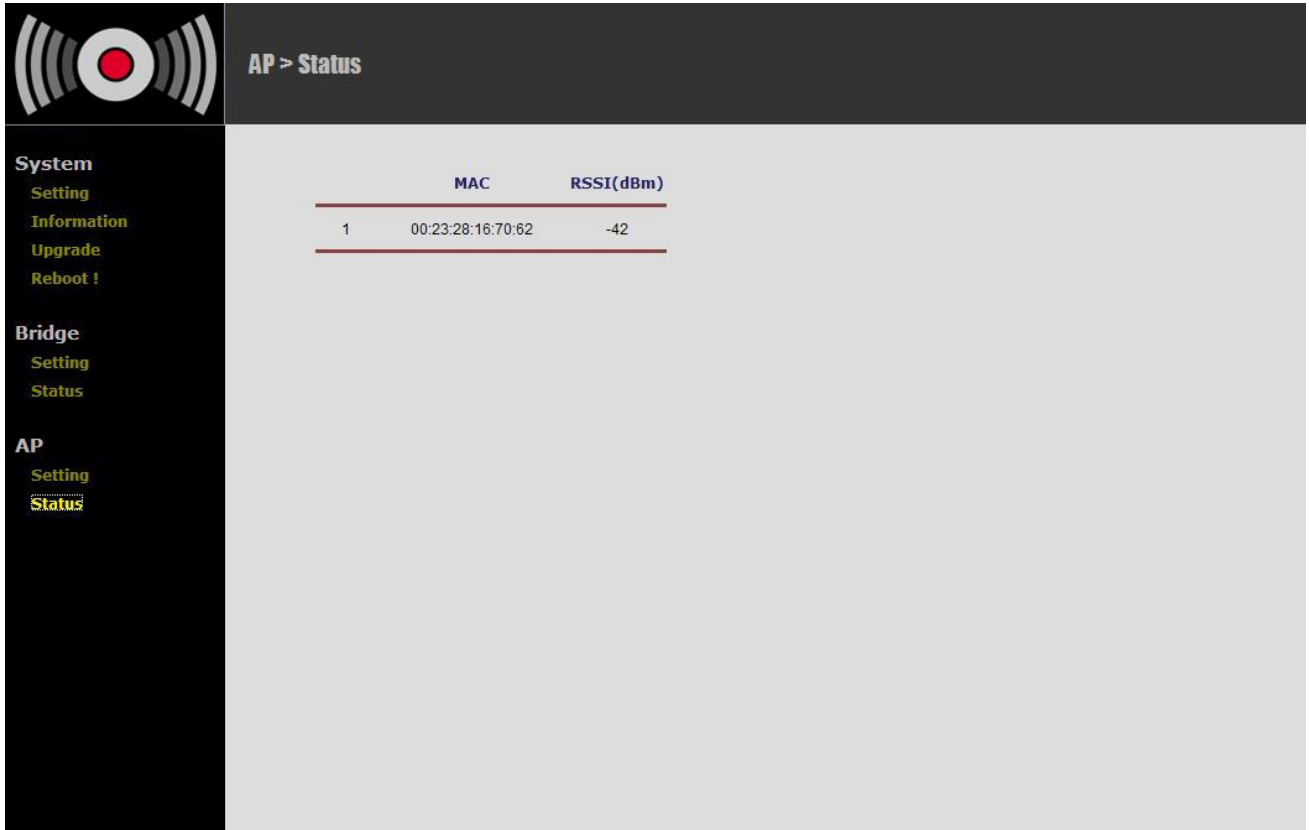
1:		16:	
2:		17:	
3:		18:	
4:		19:	
5:		20:	
6:		21:	
7:		22:	
8:		23:	
9:		24:	
10:		25:	
11:		26:	
12:		27:	
13:		28:	
14:		29:	
15:		30:	

11) To make changes take effect, click **Save** and **Reboot** when you finish all settings.



## 6.2 AP Connection Status

This page can be accessed by clicking **AP > Status**



	MAC	RSSI(dBm)
1	00:23:28:16:70:62	-42

This page can help user to identify current devices that already associated to the AP. The MAC addresses and signal strength for each client will appear.

## 7. Planning Linkage

### 7.1 Site Survey

You need to consider the following operating and environmental conditions when performing a site survey:

- **Data rates** – The sensitivity and the radio range are inversely proportional to data rates. Therefore, the maximum radio range is achieved at the lowest workable data rate, and a decrease in receiver threshold sensitivity occurs as the radio data rate increases.
- **Antenna type and placement** - Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, the radio range increases in proportion to antenna gain and height.
- **Physical environment** - Clear or open areas provide better radio range than closed or filled areas. Clear line of sight (LOS) is required to establish a good and reliable wireless link.
- **Obstructions** - Metal shelving or a steel pillar can hinder devices. Avoid placing these devices in locations where those obstructions are between the sending and receiving antennas.

### 7.2 Planning Radio Path

For the wireless communication, the Line-of-Sight (LOS) will be the major issue overbuilding up the wireless link. This evaluated procedure is to reduce the obstructions and to avoid the multiple-path signal degrading the communication quality.

The first requirement is the Line-of-Sight (LOS) between the both side Antennas. The radio line-of-sight concept is the area along the radio linking path through which is the bulk of the radio signal power travels. The area is known as the first Fresnel Zone of the radio link. For the radio link, it should avoid to be affected by obstacles in this path, including the ground within 60% of the first Fresnel Zone.

The following figure illustrates the concept of a good radio line-of-sight.

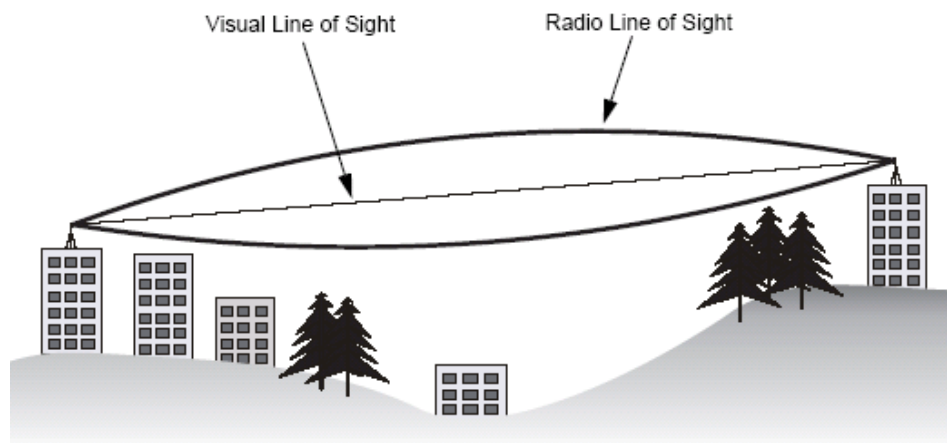


Figure 29. Line-of-Sight (LOS)

If there is any obstacle in the radio path, it may still be a radio link but the quality and the signal strength will be affected. Ensure the maximum clearance from objects on a path is important to locate the antennas and the height. For the long distance links, the radio signals might be lost partially due to the non-LOS issue.

As we setup the radio path for the wireless bridge link, it needs to consider these factors:

- Avoid any partial line-of-sight between the antennas.
- Be aware of trees that may be near the path or obstruct the path.
- Make sure there is enough clearance from buildings and there is no any building or construction blocking the path.
- Check the land topology between the antennas using topographical maps, aerial photos, or even satellite image data.
- Avoid a path that may have the temporary blockage due to the moving objects, such as cars, trains, or aircrafts.



**Note:** For the wireless link less than 500m, the IEEE 802.11a radio signal will tolerate some obstacles in the path and may not even require a visual line of sight between the antennas.

### 7.2.1 Antenna Height

The reliable wireless link usually depends on the both sides antennas for a clear radio line of sight. The minimum height is determined by the link distance, obstacles that may be in the path, topology of the terrain, and the curvature of the earth (for links over 2 miles). For the long distance links, the mast or the pole may need to be constructed to attain the minimum required height. The following table is for you to estimate the required minimum clearance above the ground or path obstruction.

Total Link Distance	Max Clearance for 60% of First Fresnel Zone at 5.8 GHz	Approximate Clearance for Earth Curvature	Total Clearance Required at Mid-point of Link
0.25 mile (402 m)	4.5 ft (1.4 m)	0	4.5 ft (1.4 m)
0.5 mile (805 m)	6.4 ft (1.95 m)	0	6.4 ft (1.95 m)
1 mile (1.6 km)	9 ft (2.7 m)	0	9 ft (2.7 m)
2 miles (3.2 km)	12.7 ft (3.9 m)	1 ft (0.3 m)	13.7 ft (4.2 m)
3 miles (4.8 km)	15.6 ft (4.8 m)	2 ft (0.6 m)	17.6 ft (5.4 m)
4 miles (6.4 km)	18 ft (5.5 m)	3 ft (0.9 m)	21 ft (6.4 m)
5 miles (8 km)	20 ft (6.1 m)	4 ft (1.2 m)	24 ft (7.3 m)
7 miles (11.3 km)	24 ft (7.3 m)	8 ft (2.4 m)	32 ft (9.7 m)
9 miles (14.5 km)	27 ft (8.2 m)	14 ft (4.3 m)	41 ft (12.5 m)
12 miles (19.3 km)	31 ft (9.5 m)	24 ft (7.3 m)	55 ft (16.8 m)

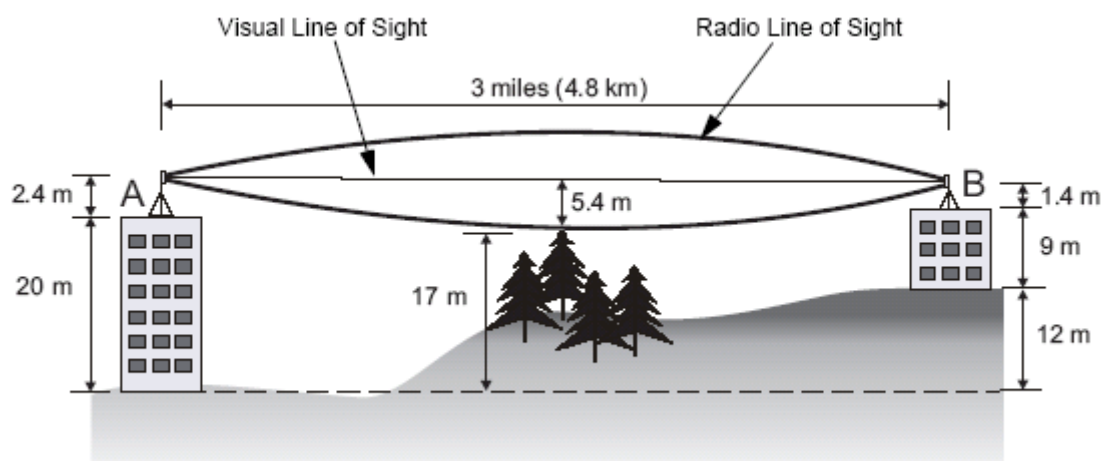


Figure 30. Antenna height

For example, the wireless link between the building A and the building B is located three miles (4.8 km) away. There is a tree-covered hill in middle. From the table above, it can be seen that for a three-mile link and the object clearance required at the mid-point is 5.4 m (17.6 ft). The tree-covered hill height

is at an elevation of 17 m (56 ft), so the antennas link on both sides need to be at least 22.4 m (73 ft) high. The building A is six stories high or 20 m (66 ft), so the mast or pole with 2.4 m (7.9 ft) must be constructed on its roof to meet the required antenna height. The building B is only three stories high or 9 m (30 ft) but it is located at an elevation that is 12 m (39 ft) higher than the building A. A mast or pole is required to mount an antenna at the required height 1.4 m (4.6ft) on the roof of building B.